IMPLEMENTATION OF (AES) ADVANCED ENCRYPTION STANDARD ALGORITHM IN COMMUNICATION APPLICATION

MOH HENG HUONG

A thesis is to submit in partial to perform of the requirement for
the award of the Degree of Bachelor Computer Science
(Computer Systems & Networking)

Faculty of Computer System & Software Engineering
UNIVERSITI MALAYSIA PAHANG

DECEMBER 2014

ABSTRACT

Internet communication has become more common in this modern world recently, and one of the important algorithms used is AES algorithm. However, most of the users have inadequate knowledge and understanding regard to this algorithm implementation in the communication field, as well as the level of security and accuracy will be questioned by the users because of the necessary to maintain the confidentiality of particular data transferred. The aim of the thesis is to provide an overview of the AES encryption algorithm, to develop a prototype that is implemented for communication purpose, and to test the developed prototype in terms of accuracy purpose. The concept of AES algorithm was firstly studied, including the definition, historical background, and a brief comparison was made between the AES algorithm with other types of algorithm. Here, the reason of choosing AES algorithm as the studied was also being explained. A prototype was consequently developed by referring to different sources, with the creation of Graphic Users Interface (GUI) by Java Swing. Fifteen files were then chosen to be the testing materials to examine the level of accuracy and security of the specific developed prototype. The obtained results show the developed prototype was able to encrypt and decrypt the file correctly without making any errors. On the basis of the results of this research, it can be concluded that the developed prototype had high accuracy and security when transferring the file between the sender and receiver that was implemented in client-server application. This research hopes to give a clear idea to the readers about AES algorithm. Further research about this topic is recommended to increase the efficiency of AES algorithm implemented in communication field, so that more different types of field can be encrypted and decrypted instead of plaintext.

ABSTRAK

Komunikasi Internet telah menjadi lebih biasa di dunia moden baru-baru ini, dan salah satu daripada algoritma penting yang digunakan ialah algoritma AES. Walau bagaimanapun, kebanyakan pengguna kurang mempunyai pengetahuan dan pemahaman tentang algoritma AES yang dilaksanakan bidang komunikasi. Secara tambahan, tahap keselamatan dan ketepatan akan dipersoalkan oleh para pengguna kerana pentingnya dalam mengekalkan kerahsiaan data tertentu yang dipindahkan. Tujuan tesis ini adalah untuk memberi gambaran keseluruhan algoritma penyulitan AES, untuk membangunkan satu prototaip yang dilaksanakan untuk tujuan komunikasi, dan untuk menguji prototaip yang dibangunkan dari segi tujuan ketepatan. Konsep algoritma AES telah dikaji pertama, termasuk definisi, latar belakang sejarah dan perbandingan ringkas telah dibuat antara algoritma AES dengan lain jenis algoritma. Di sini, sebab untuk memilih AES algoritma sebagai bahan kaji juga telah dijelaskan. Prototaip telah seterusnya dibangunkan dengan merujuk kepada sumber-sumber yang berbeza, dengan penciptaan Pengguna Grafik Interface (GUI) oleh Jawa Swing. Lima belas fail kemudiannya dipilih untuk menjadi bahan ujian untuk memeriksa tahap ketepatan dan keselamatan prototaip maju yang tertentu. Keputusan yang diperolehi menunjukkan prototaip yang dibangunkan dapat menyulitkan dan menyahsulit fail dengan betul tanpa membuat sebarang kesilapan. Berdasarkan hasil kajian ini, ia dapat disimpulkan bahawa prototaip yang dibangunkan mempunyai ketepatan yang tinggi dan keselamatan semasa memindahkan fail di antara penghantar dan penerima yang dilaksanakan pada aplikasi pelanggan-pelayan. Kajian ini diharap dapat memberikan gambaran yang jelas kepada pembaca mengenai algoritma AES. Penyelidikan lanjut mengenai topik ini adalah disyorkan untuk meningkatkan kecekapan algoritma AES dilaksanakan dalam bidang-bidang yang lain juga boleh disulitkan dan dinyahsulit hanya dalam bentuk teks.

TABLE OF CONTENTS

CHAPTER 3 RESEARCH METHODOLOGY

CHAPTER 4 DESIGN

CHAPTER 5 IMPLEMENTATION

CHAPTER 6 RESULT AND DISCUSSION

CHAPTER 7 CONCLUSION

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 ENCRYTION ALGORITHM IN TWO-WAYS COMMUNICATION

In this developing 21st Century, computer has become the important channel for people to communicate each other, by sending, receiving, writing, editing, uploading and downloading through web. However, the security issue may arise with this internet communication. They may worry whether the files and data will be sent in a secure way or not? Thus, it has to be the compulsory which all the files and data sent through the web need to be secured and protected because everybody is concerned about the sensitive data to the web and most organizations believe that web is not as safe as their own data centres. Imagine that how much it data or information might be worth going? So others more professional person was already knew this kind of problem will be bringing in web so they had investigative kind of encryption algorithm to solve this problem. Hence, an encrypted communication can be achieved that is available between sender and receiver, without being seen or attacked by the unauthorised third party.

There are few security encryption algorithms available such as 3DES, Advanced Encryption Standard (AES), Blowfish, Data Encryption Standard (DES), and International Data Encryption Algorithm (IDEA) and so on (Patrick D, Gallagher, 2014).

1.2 PROBLEM STATEMENT

Nowadays, internet has become one of the important part in our lives and it is considered as one of the communication way. Our lives will be unpleased if there is no internet. Although the internet are widely used globally, it is believable some people may still not know the process involved in the internet communication, and one of the example processes behind the internet is the Advanced Encryption Standard (AES) encryption to encrypt and decrypt the file and chat by coding.

Starting from the existence of computer until now, there are lots of communications by sending or receiving the data or files between the sender and receiver. Meanwhile, the encryption process is executed with the communication to protect the data or file transmission, thus, only the receiver can understand the content inside the file and data sent by the sender, which is a two-ways communication in secure way.

Besides, some of the people may worry about the accuracy of this encryption process where some errors may occur when encrypting the data and doing translation to the receiver, in order to prevent the wrong interpretation of the receiver (Sri Vallabh et al., 2013).

Based on the motivations mentioned above, the following are the research questions:

i. How to study this AES encryption so that it will be more understand by the readers?
ii. How to develop the prototype for AES encryption with correct process of encryption and decryption the data and file?

1.3 RESEARCH OBJECTIVE

There are three major objectives of the research:

i. To study the AES encryption algorithm.
ii. To develop an AES algorithm prototype for implementing it in client-server application with communication purpose.
iii. To test the AES encryption and decryption by the prototype.

1.4 SCOPE

The scope of this research is mainly about the AES algorithm, including the introduction, history and cryptography process which covers the working principle, followed by development of a prototype on communication application. Moreover, the quality test on the prototype developed, regarding on the security and data encryption process in the application, with different types of web browser.

I. Application security testing

All the data sent or received by using this algorithm system must be protected from data thieves' or any attackers in order to maintain the confidentiality or secrecy. In other words, there is only allowed the authenticated or verified identity sender and receiver can interpret the message by encrypting and decrypting the data respectively.

II. Online application

One of the most common application use AES encryption is modern email programme. It is undeniable that the choice of e-mail client is the priority consideration to identify what type of AES encryption used, as long as it is afforded by the server. For example, it is tested and concluded that 128-bit AES is good in Outllook 2007 (email programe) applied in Windows Vista (operating system). Thus, in this research, the AES encryption focuses on the how to do the plaintext, that can be either number or text, to encrypt it into a cipher text for consequently decrypting purpose, which is applied in various online application uses.

1.5 THESIS ORGANIZATION

This thesis consists of seven chapters:

Chapter 1: It is to discuss on introduction of Using Advanced Encryption Standard (AES) Algorithm in communication application.

Chapter 2: It is to describe the each research of literature review about AES encryption algorithm.

Chapter 3: This is to describe my research methodology, which was the step involved in developing this project in clear sequence.

Chapter 4: It is to design the prototype to implement AES encryption algorithm.

Chapter 5: It discussed the process and systematic to implement the AES encryption algorithm in communication application.

Chapter 6: Chapter shows the result after testing and discussion as well as the research constraints.

Chapter 7: This chapter gives the epilogue, limitations, and whole research summary.

CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

In this chapter, the information related to the AES encryption algorithm was described by referring to variety of literature through different type of resources. As an overview, this chapter consisted of five main sections. First, section 2.1 described the overview or historical background of AES. Secondly, the definition for AES was explained in Section 2.2, followed by the comparison between different types of encryption algorithm in terms of advantages and disadvantages in Section 2.3. Next, Section 2.4 listed the differences between AES, DES, 3DES and BLOWFISH. This chapter was ended with summary made regarding the reasons of choosing AES algorithm in this project for communication in Section 2.5.

2.2 OVERVIEW / HISTORICAL BACKGROUND

In 1997, United States National Institute of standards and technology (NIST), which is a branch of United States Government, began processes to identify replacement for the Data Encryption Standard (DES). DES is currently considered safe due to the progress in computer processing power. NIST's goal is replacing the definition with the US Government for non-military applications of information security of DES. For sure, it was recognized that commercial and other non-governmental users will benefit from NIST standards of work and work as a business.

NIST invites encryption and data security experts from around the world to participate in the discussion and selection process. Five encryption algorithms have been adopted for the study. Through the process of reaching consensus from Belgium cracked by Joan Daeman and Vincent Rijmen presented an encryption algorithm was selected it. Daeman and Rijmen used before choosing the name (exported from its name) of the Rijndael algorithm. So the original name for AES algorithm was Rijndael algorithm. However, the algorithm was subsequently given a name with Advanced Encryption Standard (AES), which is commonly used from ancient until today.

On 2000 NIST's AES encryption algorithm has been formally adopted and published it as the designated federal standard under FIPS 197. As expected, the encryption software had many vendors have incorporated into their products and hardware AES encryption (Townsend Security, 2007).

The summary of AES selection processes are shown as follows Rijndael Algorithm (2011):

I. 12/09/1997: the NIST publicly calls for nominees for the new AES

II. 20-23/08/1998: AES conference for 15 algorithms are candidates for becoming AES

- This is in public mode give them to review of the algorithm

III. 22-23/03/1999: AES conference with doing presentation, analysis and testing the algorithm

IV. 09/08/1999: the 5 finalists are announced out to final selection with public review

- MARS, RC6, RINJDAEL, SERPENT, TWOFISH

V. 13-14/04/2000: AES conference from the 5 finalists algorithm with activities presentation, analysis and testing

VI. 02/10/2000: the winner is chosen: RINJDAEL

VII. 28/02/2001: Federal Information Processing Standard(FIPS) gave publication of a draft for 90 days and proposal to the Secretary of Commerce for approval

VIII. 06/12/2001: Publication on the Federal Register and starting effectively from May 26, 2002

2.3 DEFINITION

The Advanced Encryption Standard (AES) encryption algorithm had some several of itself definition and explanation but all the definition and explanation is established by National Institute of Standards and Technology (NIST) (Patrick D, Gallagher, 2014).

In this overview will discuss three types of AES's definition and explanation from three different sources. Firstly, the AES is kind of formal encryption technique that had already accepted by worldwide. AES is one kind of the block cipher encryption algorithm; it uses the encryption key to encrypt a few rounds. So a block cipher is an encryption algorithm in a single data block. Standard AES encryption algorithm block are 128 bits or 16 bytes in length, 192bits or 24bytes and 256 or 32bytes (Vincent Rijmen, et al., 2014).

Others way to define the advanced encryption standard (AES) is a specification for the electronic data in encryption (Vincent Rijmen et al., 2014). Again AES encryption is an algorithm used to encrypt as well as decrypt data electronic transmission of data protection purposes. Moreover, AES algorithm allows the use of cipher key that are 128, 192, or 256 bits long and also that are to protect the 16-byte blocks in the data encryption key (Silicon, 2011).

With AES encryption and decryption are implemented using the same key so this is called a symmetric encryption algorithm. While encryption algorithm uses in two different keys, that are one public and one private which it is called asymmetric encryption algorithm. The data encryption key is used in the encryption process is a binary string. It is because those are using the same encryption key to encrypt and decrypt the data, it is important to keep a secret encryption key, and use the keys hard to guess. Some key generation software used for this particular task. Another method is derived from a passphrase key. While a good encryption system was never used separate passphrase as the encryption key (Townsend, 2007).

2.4 TYPES OF ENCRYPTION ALGORITHM & EACH ADVANTAGES AND DISADVANTAGES

2.4.1 DATA ENCRYPTION STANDARD (DES)

Data Encryption Standard (DES), this is the first time encryption standard by the NIST (United States National Institute of standards and technology) recommended in early 1970s. This DES algorithm is proposed by IBM while other names call LUCIFER (Abdel-Karim Al Tamimi, 2013). DES that is Data Encryption Standard is used 56-bits key and 16 cycle through each key is ranked 48 submarines formed by 56-bit key. When it is decryption, Sub-key in reverse order and it will use the same algorithm. 64-bit block size is L and R block of 32 bits (Milind Mathur et al., 2013).

Certainly, there are advantages and disadvantages of DES algorithm. Advantages of DES are it is more fast process in hardware and comparatively fast in software, DES is more easily to learn the details as well as implement it and every five years the Government (United States) will required to renew the certify because this is their official Government standard. While disadvantages of DES are outdated because technology nowadays is more improving every minute by minutes so it is a chance to break the encrypted code. Then, it is slow when implement in software because it not designed for software and it cannot be decrypt the data (Cipher text) if we lost that secret key (Priya Kapoor et al., 2012).

2.4.2 TRIPLE DES

Triple DES another name is 3DES was proposed is one algorithm that is enhancement of DES (Abdel-Karim Al Tamimi, 2013). And an IBM team is developed it around 1974 while in 1977 it is adopted become standard in national. The triple DES algorithm for just three times in a row with three different keys should be used for expanding the size of DES keys. Combinations to 168-bit key size (3 x 56) have no access to power (Abdel-Karim Al Tamimi, 2013).

So the advantages of Triple DES are easily to implement inside both of the hardware and software application, more universal in libraries and most systems and also to fix the weaknesses of DES. In addition, the disadvantages of 3DES are not support larger key size, not faster implement in both software and hardware and also outdated when the technology is more increasing and also improving fast (Quora, 2014).

2.4.3 BLOWFISH

In this algorithm that is provided by Bruce Schneier and it is a domain encryption that most common public. Blowfish is 64-bit algorithm block cipher with a variable length key. So the Blowfish is burn on 1993 that start introduced through publication. This algorithm can be executed on hardware application while mostly it is used in software application refer to Abdel-Karim Al Tamimi (2013). BLOWFISH, it is aim to replace the DES algorithm. From 32 bits to 448 bits, use a variable-length key. Blowfish patents and licenses are not available for free, and can be used free of charge for all. Blowfish is a fast block cipher is one of the most developed to date (Milind Mathur et al., 2013).

The advantages of Blowfish are it is support larger size of key length (32-448 bits), it is a fast block cipher but not included changing keys and there are freely to everyone to used it because it's not set any patents. Another perspective disadvantages are it is not suitable to encrypt the files size 4 GB and not secure if users choosing a weak keys become their secret keys (Bruce Scheier, 2009).

2.4.4 ADVANCED ENCRYPTION STANDARD (AES) / RIJNDAEL ALGORITHM

The Advanced Encryption Standard (AES), this is a symmetric block cipher that uses a symmetric key can be 128, 192, or 256 data blocks of 128 bits encryption. AES encrypted the data block when process encryption in 10, 12 and 14 rounds that it depend on the key size. AES encryption is fast and flexible (Milind Mathur et al., 2013)

Otherwise, the advantages of AES are faster executed in both of the hardware and software, it is the latest that required by United States and International Standards and also more securely to use, lastly it support a larger key sizes than others algorithm. Then, disadvantages of AES are difficult to know the details of process because it is too patents encryption and it will difficult to decrypt the data (Cipher text) if lost the secret (private) keys (Quora, 2014).

2.5 COMPARISON ON AES, DES, 3DES AND BLOWFISH

Actually there were a lot of encryption algorithms in our environment but now just take three most popular encryption algorithms to do some comparison among them. The following is the table of comparison of AES, DES, 3DES and Blowfish.

Table 2.1: Comparison between AES, DES, 3DES and BLOWFISH

FACTORS	AES	DES	3DES	BLOWFISH
Key Length	128, 192, or 256 bits	56 bits	(K1, K2, and K3) 168 bits (K1 and K2 is same) 112 bits	32-448 bits
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Symmetric Cipher Algorithm
Block Size	128, 192, or 256 bits	64 bits	64 bits	64 bits
Developed	2000	1977	1978	1993
Cryptanalysis Resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Vulnerable to differential, brute force attacker could be analyze plaint text using differential cryptanalysis	Vulnerable to differential, brute force attacker
Security	Consider secure	Proven Inadequate	One only weak which is exit in DES	vulnerable
Possible Keys	2^{128}, 2^{192}, or 2^{256}	2^{56}	2^{112}, or 2^{168}	2^{32}, 2^{448}
Possible ASCII Printable Character Keys	95^{16}, 95^{24}, or 95^{32}	95^{7}	95^{14}, or 95^{21}	95^{4}, 95^{56}
Time Requirement To Check All Possible Keys At 50 Billion Keys Per Second**	For a 128-bit key: 5×10^{21} years	For a 56-bit key: 400 days	For a 112-bit key: 800days	For a 448 bit key: 10^{116} years
Rounds	10(128-bits), 12(192-bits), 14(256-bits)	16	48	16
Key(s)	Single	Single	Single (later divided in 3 parts)	Public

2.6 SUMMARY

Taken as a whole for this chapter, it concluded that AES-128 bits encryption algorithm was chosen to be the choice of this research material using in communication. This is because AES algorithm is updated time by time and it has been already used by U. S. Government Standard encryption algorithm for encrypting electronic information and replacing DES and 3DES as well. In addition, it is the most frequently used algorithm, compared to other types of algorithm. Apart from that, AES algorithm had the advantage of more secure encrypted communication when compared to others encryption algorithm. The encrypted and decrypted data was it unbreakable from the beginning until today by using AES algorithm. Lastly, it was needed to test the accuracy of AES algorithm in encrypting or decrypting the data, whether the plaintexts were correctly processed or not in communication between the sender and receiver, so that the information can be transferred in a more secure and correct way.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter would going to describe the research methodology used in the developing the AES-128 bit encryption algorithm for web security. In section 3.2, a flow chart about the review on this research paper was made to know the implementation steps used in this research. The following section 3.3 and 3.4 described on the types of study methods used, and definition was given, together with analysis of AES encryption algorithm was done, respectively. In section 3.5, the AES encryption algorithm in which version was chosen, followed by giving description on AES-128bit encryption used to encrypt and decrypt the text in section 3.6. Next, Section 3.7 showed the research methodology of proposed technique to develop a prototype for AES-128bit. Meanwhile, both section 3.8 and 3.9 would consequently surmise the initial experiment result and expected result. In section 3.10, different types of hardware and software used in this research were shown and explained clearly in table form. At last, the initial experimental results were obtained after the experiment and shown in section 3.4.

3.2 FLOW CHART

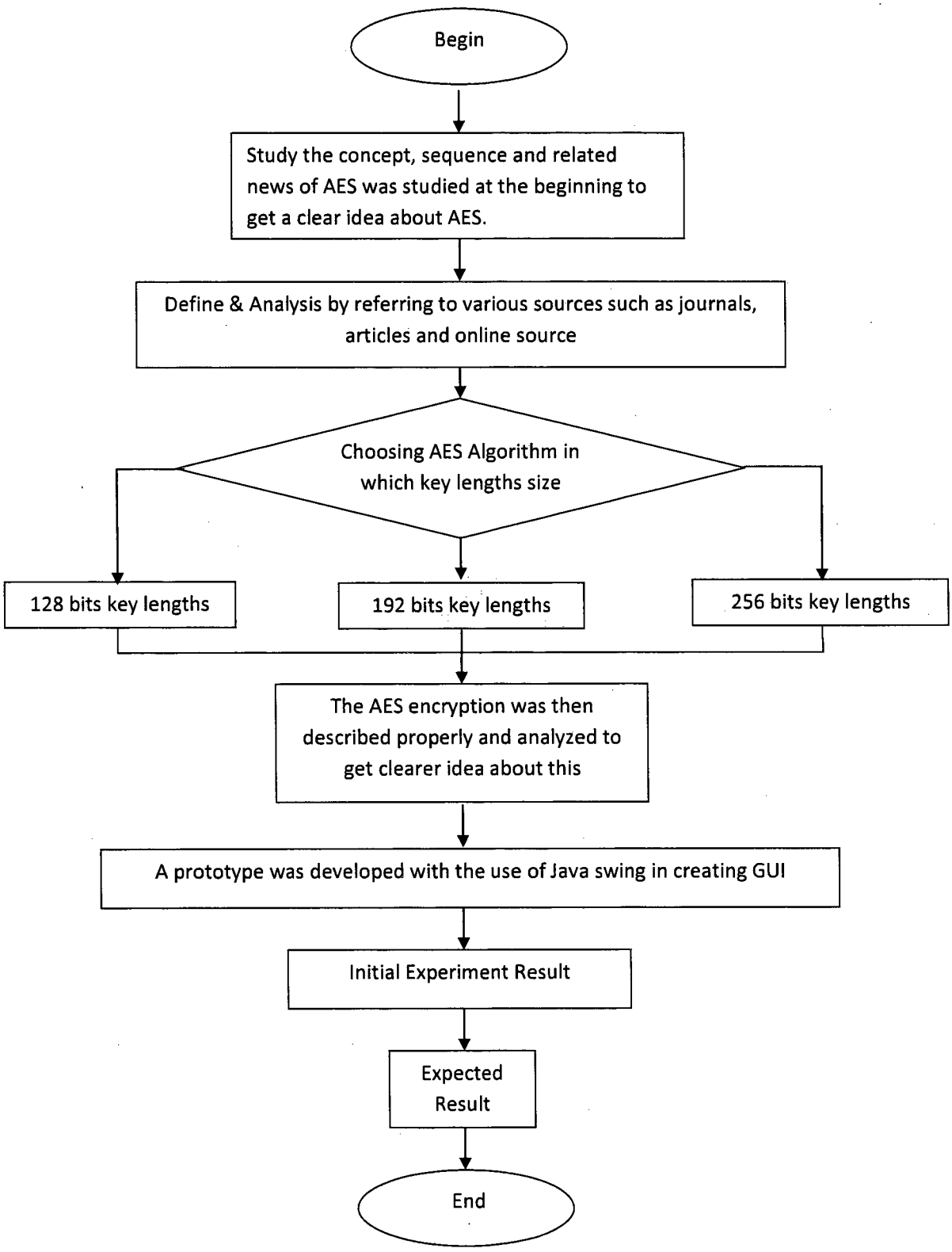

Figure 3.1: Research activity flow chart

3.3 STUDY AES ENCRYPTION ALGORITHM

Generally, the first step was probably most important turn to start in this research. Before and simultaneously started this research, lots of information were searched and read by referring variety of sources, which are articles, thesis and book that discuss about kind of encryption algorithm used behind web. Thus, more knowledge on AES algorithm was gained after this searching. At the same time, different types of encryption algorithm used in enterprise nowadays were identified. After that, the latest market was studied to know what kind of encryption that usually used in their business, hardware, software or network. Besides that, the objectives of this research, problem statements and scope were identified and explained clearly in the first part of this research. But at the final, AES algorithm would be most regarding on because AES encryption was needed to develop in this research.

3.4 DEFINE & ANALYSIS AES ENCRYPTION

In this step, the AES encryption algorithm was studied comprehensively, especially the definition and concepts or working principles applied, in order to define and understand it clearly. For example, AES encryption is one of the standard notices the Rijndael Algorithm, it was a symmetric algorithm block cipher. After that, can be process data blocks of 128 bits by using cipher keys with lengths of 128-bits, 192-bits, and 256-bits. Meanwhile, an analysis about AES encryption was done because in this algorithm might be use in three different kind of key lengths, therefore these different "season" might referred as "AES-128bits", "AES-192bits", and AES-256bits" and number of rounds for each of them were 10, 12 and 14. Furthermore, the advantages and disadvantages of AES encryption were also being analyzed, followed by making a comparison of AES algorithm with others types of encryption.